					Fügen Sie hier den Namen der eingetragenen juristischen Person ein							
Dokumentnummer: P11					Dokumenttitel: **Richtlinie zur Verwaltung von Benutzerkonten und Berechtigungen**							
Version: 1.0		Datum des Inkrafttretens: 01.01.2025			Dokumentenverantwortlicher:							
X	Richtlinie		Standard		Verfahren		Formular		Register		Sonstiges	

Änderungshistorie				
Änderungsnummer	**Änderungsdatum**	**Änderungen**	**Geprüft von**	**Prozessverantwortlicher**

Genehmigungen			
Name	**Position**	**Datum**	**Unterschrift**

An Standards und Vorschriften ausgerichtet

Standard/Vorschrift	Klausel/Artikel	Kommentar
ISO/IEC 27001:2022	Klausel 6.1.3, Klausel 8	-
ISO/IEC 27002:2022	Maßnahmen 5.15-5	-
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2 - IA-5, AU-2, AU-12	-
EU-DSGVO	Artikel 5(1)(f), 32; Erwägungsgrund 39	-
EU NIS2	Artikel 21(2)(a, d), 21(3)	-
EU DORA	Artikel 5, 9	-
COBIT 2019	DSS01, DSS05, APO	-

1. Zweck

1 Diese Richtlinie legt verbindliche Kontrollen für die Verwaltung von Benutzerkonten und Berechtigungen in allen Informationssystemen und Diensten fest. Sie stellt sicher, dass der Zugriff auf organisatorische Ressourcen auf Grundlage einer validierten Identität, eines nachgewiesenen Bedarfs für die jeweilige Rolle sowie der Prinzipien der minimalen Rechtevergabe und Funktionstrennung gewährt wird.

1.1 Sie unterstützt die Verpflichtung der Organisation zur Informationssicherheit durch die Einführung strukturierter und auditierbarer Prozesse für die Bereitstellung von Konten, die Zuweisung von Berechtigungen, die Überwachung der Nutzung und den Entzug von Benutzerkonten.

1.2 Diese Richtlinie ist wesentlich, um das Risiko unbefugter Zugriffe, des Missbrauchs von Berechtigungen, von Insider-Bedrohungen sowie der Nichteinhaltung anwendbarer regulatorischer Rahmenwerke zu reduzieren.

2. Geltungsbereich

2.1 Diese Richtlinie gilt für alle Beschäftigten und Auftragnehmer, Drittanbieter, Berater sowie sonstige Personen, denen Zugriff auf die IT-Ressourcen, Anwendungen oder Daten der Organisation gewährt wird.

2.2 Sie regelt alle Systeme und Umgebungen, in denen Mechanismen zur Benutzerauthentifizierung und Zugriffskontrolle angewendet werden, einschließlich, aber nicht beschränkt auf:

2.2.1 Unternehmensanwendungen und Datenbanken

2.2.2 Cloud-Plattformen und SaaS-Umgebungen

2.2.3 Betriebssysteme und Administrationskonsolen

2.2.4 Fernzugriffswerkzeuge und VPNs

2.2.5 Systeme für das Identitäts- und Zugriffsmanagement (IAM)

2.3 Die Richtlinie umfasst sowohl Standardbenutzerkonten als auch privilegierte Benutzerkonten und schließt Kontrollen zu folgenden Themen ein:

2.3.1 Erstellung, Änderung und Deaktivierung von Konten

2.3.2 Rechteausweitung und Delegation

2.3.3 Sitzungssteuerung und -überwachung

2.3.4 Authentifizierungsmethoden und Verwaltung von Zugangsdaten

3. Ziele

3.1 Sicherzustellen, dass alle Benutzerkonten eindeutig identifizierbar, ordnungsgemäß autorisiert und erst nach formaler Prüfung des Bedarfs zugewiesen werden.

3.2 Die Prinzipien der minimalen Rechtevergabe umzusetzen und unnötige oder übermäßige Zugriffe zu verhindern, indem für die Vergabe und Nutzung privilegierter Konten strenge Kontrollen durchgesetzt werden.

3.3 Zeitnahe Aktualisierungen des Kontostatus auf Grundlage von Änderungen im Beschäftigungs- oder Vertragsverhältnis oder bei Rollenänderungen zu verlangen, einschließlich der unverzüglichen Deaktivierung bei Beendigung des Beschäftigungs- oder Vertragsverhältnisses.

3.4 Die proaktive Erkennung und Behebung inaktiver, missbräuchlich genutzter oder unbefugter Konten durch Protokollierung, Überprüfungen und Automatisierung zu ermöglichen.

3.5 Die Ausrichtung an ISO/IEC 27001:2022 und zugehörigen Standards aufrechtzuerhalten und Verpflichtungen aus einschlägigen gesetzlichen und regulatorischen Rahmenwerken wie DSGVO, NIS2, DORA und COBIT 2019 zu erfüllen.

4. Rollen und Verantwortlichkeiten

4.1 Chief Information Security Officer (CISO)

4.1.1 Ist Eigentümer dieser Richtlinie und stellt ihre Durchsetzung in der gesamten Organisation sicher.

4.1.2 Prüft und genehmigt formale Ausnahmen oder Fälle von Notfallzugriff.

4.1.3 Berichtet kontobezogene Audit-Feststellungen und eskaliert Risiken an die Geschäftsleitung.

4.2 Verantwortlicher für Zugriffskontrolle / IT-Administrator

4.2.1 Betreibt und pflegt die technischen Kontrollen für das Management des Lebenszyklus von Benutzerkonten.

4.2.2 Führt nach genehmigter Anforderung Maßnahmen zur Bereitstellung, zum Entzug von Zugriffsberechtigungen und zur Berechtigungsverwaltung aus.

4.2.3 Führt ein maßgebliches Register aller Benutzerkonten, ihres Status und ihrer Berechtigungsstufe.

4.2.4 Unterstützt Audits und Compliance-Überprüfungen durch Protokolle und Aktivitätsberichte.

[... Abschnitte 4.3–8 sind in dieser Vorschau nicht enthalten. Erwerben Sie das vollständige Dokument, um auf den gesamten Inhalt zuzugreifen. ...]

9. Anforderungen an Überprüfung und Aktualisierung

9.1 Diese Richtlinie ist mindestens jährlich oder bei wesentlichen Änderungen in folgenden Bereichen zu überprüfen:

9.1.1 Organisationsstruktur oder Geschäftsprozesse

9.1.2 IT-Systeme, Identitätsplattformen oder Zugriffsmethoden

9.1.3 Regulatorische oder vertragliche Anforderungen im Zusammenhang mit Identitäts- und Zugriffsmanagement

9.2 Der Chief Information Security Officer (CISO) ist gemeinsam mit dem Verantwortlichen für Zugriffskontrolle dafür verantwortlich, den Überprüfungsprozess einzuleiten und die Rückmeldungen der relevanten Interessengruppen zu koordinieren.

9.3 Anlassbezogene Überprüfungen können ausgelöst werden durch:

9.3.1 Sicherheitsvorfälle im Zusammenhang mit Kontenmissbrauch

9.3.2 Audit-Feststellungen, die Mängel im Management des Kontenlebenszyklus aufzeigen

9.3.3 Einführung neuer Werkzeuge für Identitätsmanagement oder Privileged Access Management (PAM)

9.4 Aktualisierungen dieser Richtlinie müssen:

9.4.1 Versionskontrolliert sein und in der ISMS-Dokumentationsbibliothek erfasst werden

9.4.2 Allen relevanten Interessengruppen mitgeteilt werden, einschließlich Abteilungsleitern, IT-Betrieb und HR

9.4.3 Durch aktualisierte Schulungsunterlagen und Verfahrensanweisungen unterstützt werden

9.5 Alle Änderungen müssen von der Geschäftsleitung oder dem Informationssicherheitslenkungsausschuss genehmigt und für Audit-Zwecke protokolliert werden.

10. Zugehörige Richtlinien und Verknüpfungen

10.1 Diese Richtlinie ist operativ mit den folgenden zugehörigen Richtlinien innerhalb der ISMS-Suite verknüpft und wird durch diese unterstützt:

10.1.1 P4 Richtlinie zur Zugriffskontrolle: Legt die übergeordneten Prinzipien und Mechanismen der Zugriffskontrolle fest, einschließlich regelbasierter und rollenbasierter Kontrollen.

10.1.2 P7 Richtlinie für Onboarding und Austritt: Beschreibt die Verfahrensschritte zur Einrichtung und Beendigung von Benutzerzugriffen im Einklang mit HR-Maßnahmen.

10.1.3 P8 Richtlinie zur Sensibilisierung und Schulung für Informationssicherheit: Stärkt die Verantwortlichkeiten der Benutzer für Kontensicherheit und den Schutz von Zugangsdaten.

10.1.4 P13 Richtlinie zur Datenklassifizierung und Kennzeichnung: Steuert Zugriffsrechte auf Grundlage der Datenklassifizierung und stellt sicher, dass Berechtigungsgrenzen den Sensibilitätsstufen entsprechen.

10.1.5 P22 Richtlinie zur Protokollierung und Überwachung: Stellt sicher, dass Prüfpfade für alle kontobezogenen Aktivitäten erfasst und zur Erkennung von Anomalien oder unbefugter Nutzung überprüft werden.

10.1.6 P30 Incident-Response-Richtlinie (P30): Regelt Eskalation, Eindämmung und Maßnahmen nach einem Vorfall bei Missbrauch von Berechtigungen oder unbefugten Kontenaktivitäten.

10.2 Diese Richtlinien wirken zusammen, um ein kohärentes, risikobasiertes Rahmenwerk für Identitäts- und Zugriffsmanagement in der gesamten Organisation durchzusetzen.

11. Referenzstandards und Rahmenwerke

11.1 Diese Richtlinie ist an global anerkannten Cybersicherheitsstandards und regulatorischen Rahmenwerken ausgerichtet, die ein sicheres Management von Identitäten, Zugriffen und Berechtigungen als Kernbestandteil der Informationssicherheit einer Organisation verlangen.

11.2 ISO/IEC 27001:

11.2.1 Klausel 6.1.3 verlangt von Organisationen, Informationssicherheitsrisiken zu bestimmen, zu bewerten und zu behandeln. Dadurch wird die Verwaltung von Zugriffen und Berechtigungen als formale, risikobasierte Kontrolle in den Planungsprozess des ISMS eingebettet.

11.2.2 Klausel 8.1 - Betriebliche Planung und Steuerung: Verstärkt die Umsetzung technischer und verfahrensbezogener Schutzmaßnahmen, die Benutzerzugriffe und privilegierte Zugriffe regeln.

11.3 ISO/IEC 27002:2022 - Maßnahmen 5.15 bis 5:

11.3.1 Maßnahme 5.15 - Benutzerzugriffsverwaltung: Unterstützt formale Prozesse für Kontobereitstellung, Zugriffsgenehmigung und regelmäßige Überprüfung von Zugriffsrechten.

11.3.2 Maßnahme 5.16 - Identitätsmanagement: Legt die Eindeutigkeit von Identitäten, Kontrollen über den Lebenszyklus und die Durchsetzung sicherer Authentifizierung fest.

11.3.3 Maßnahme 5.17 stellt sicher, dass die Zuweisung und Nutzung privilegierter Zugriffsrechte streng kontrolliert, nachvollziehbar und im gesamten Kontenlebenszyklus an dem Prinzip der minimalen Rechtevergabe ausgerichtet werden.

11.3.4 Maßnahme 5.18 - Privilegierte Zugriffsrechte: Wird durch rollenbasierte Zuweisung von Berechtigungen, Auditierung und Anforderungen an die Genehmigung erhöhter Zugriffe vollständig abgedeckt.

11.4 Diese Maßnahmen leiten die strukturierte Umsetzung von Kontoregistrierung, Deregistrierung, Trennung von Berechtigungen und Nutzung von Authentifizierungsinformationen. Die Richtlinie setzt Governance für den Lebenszyklus von Identitäten, Just-in-Time-Zugriff und die Überwachung erhöhter Sitzungen durch, um unbefugte Systemnutzung zu verhindern.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (Richtlinie zur Zugriffskontrolle) und AC-2 (Kontenverwaltung): Werden durch Richtlinienvorgaben zu Zugriffsgenehmigungen, Rollenzuordnung und Auditierung von Benutzerkonten abgebildet.

11.5.2 AC-5 (Funktionstrennung) und AC-6 (Prinzip der minimalen Rechtevergabe): Werden durch Beschränkung von Berechtigungen, Ausrichtung an Aufgabenrollen und Doppelgenehmigung für Hochrisikoaufgaben erfüllt.

11.5.3 IA-2 bis IA-5 (Identifizierung und Authentifizierung): Werden durch starke Authentifizierungsmechanismen, Regeln für den Lebenszyklus von Zugangsdaten und Anforderungen an die Multi-Faktor-Authentifizierung durchgesetzt.

11.5.4 AU-2, AU-12 (Audit-Protokollierung und Analyse): Werden durch Sitzungsaufzeichnung und Überwachung privilegierter Aktivitäten in sensiblen Umgebungen adressiert.

11.6 EU-DSGVO (2016/679):

11.6.1 Artikel 32 - Sicherheit der Verarbeitung: Verlangt Zugriffskontrollen und Mechanismen zur Identitätsprüfung zum Schutz personenbezogener Daten. Dies wird durch verpflichtende Kontogenehmigungen, Berechtigungsüberprüfungen und starke Authentifizierungsschutzmaßnahmen erfüllt.

11.6.2 Artikel 5(1)(f) - Integrität und Vertraulichkeit: Stellt sicher, dass auf personenbezogene Daten nur von autorisierten Benutzern mit legitimen Rollen zugegriffen wird; dies wird durch die Durchsetzung dieser Richtlinie zur Kontenverwaltung gestützt.

11.6.3 Erwägungsgrund 39: Verlangt eine klare Zugriffsbeschränkung und Rechenschaftspflicht. Diese Richtlinie unterstützt die vollständige Nachvollziehbarkeit von Benutzeridentitäten und Berechtigungszuweisungen.

11.7 EU-NIS2-Richtlinie (2022/2555):

11.7.1 Artikel 21(2)(a, d): Verlangt von Einrichtungen die Durchsetzung von Richtlinien zur Zugriffsverwaltung sowie den sicheren Umgang mit Zugangsdaten und privilegierten Sitzungen; dies wird durch die in dieser Richtlinie festgelegten Kontrollen zur Bereitstellung, Überwachung und Ausnahmebehandlung unterstützt.

11.7.2 Artikel 21(3): Fördert Zugriffsdisziplin und eine hohe Sicherheit der Identitätsfeststellung in kritischen Sektoren; dies wird durch die Verwendung eindeutiger Kennungen, RBAC und zeitlich befristeten erhöhten Zugriff erfüllt.

11.8 EU DORA (2022/2554):

11.8.1 Artikel 5 - IKT-Governance und Kontrolle: Verlangt formalisierte Prozesse für das Management von IKT-Benutzern, die durch dokumentierte Bereitstellung, Deaktivierung und Ausnahmebehandlung abgedeckt werden.

11.8.2 Artikel 9 - Management von IKT-Risiken: Verpflichtet Organisationen, Systeme durch Zugriffsbeschränkungen und Überwachung abzusichern; dies wird durch Multi-Faktor-Authentifizierung, Protokollierung privilegierter Zugriffe und zentralisierte Überprüfungen umgesetzt.

11.9 COBIT 2019:

11.9.1 DSS01 - Gesteuerte Betriebsabläufe: Fördert die Durchsetzung standardisierter betrieblicher Kontrollen, einschließlich Management des Kontenlebenszyklus und Zugriffsdokumentation.

11.9.2 DSS05 - Sicherheitsdienste verwalten: Spiegelt die sichere Verwaltung von Benutzer- und Systemberechtigungen wider und unterstützt die Risikominderung durch das Prinzip der minimalen Rechtevergabe und die Validierung des Prüfpfads.

11.9.3 APO13 - Gesteuerte Sicherheit: Verlangt Zugriffsgovernance über digitale Assets hinweg; dies wird durch formalisierte Verfahren zur Autorisierung von Konten und Rollen mit regelmäßigen Überprüfungspflichten erfüllt.